BROCADE

Brocade Network Advisor 11.1.2
Release Notes v1.0

53-1002124-06 Rev A

November 18, 2011

Document History

Document Title	Summary of Changes	Publication Date
Brocade Network Advisor 11.1.2 Release Notes v1.0	Initial release	November 18, 2011

© 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, DCX, Fabric OS, and SAN Health are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd.*

Export of technical data contained in this document may require an export license from the United States Government.

Contents

Overview 5
Software Feature Overview 5
SAN and IP Management Feature Enhancements 5
IP Management Feature Enhancements 5
SAN Management Feature Enhancements 5
Migrations & Upgrades 6
Operating Systems Supported 6
Device Platform & Hardware Support Requirements 7
Installing Network Advisor 10
To install Network Advisor on Windows (Server) 10
To install Network Advisor on Linux (Server) 10
To launch the Network Advisor Client 10
Installation Notes 11
Important SAN Notes 11
Miscellaneous Important Notes that Apply to SAN Installations 11
Removing Switches 11
Secure Fabric OS fabrics cannot be discovered from Network Advisor 11
Display of Logical Switches 11
Destination columns are blank for Brocade Encryption Switch in top talkers dialog 12
Firmware Download through SCP Server 12
DCFM to Network Advisor remote migration is not supported 12
Important IP Notes 12
Miscellaneous Important Notes that Apply to IP Installations 12
IP Address and Detailed Reports 12
Properties Dialog Sorting and Selection can map to incorrect port / product 12
Image Backup with SCP 12
Linux and Windows OS: INM to INM Server Cloning for Network Advisor Migration 12
Boot, Monitor, Firmware Image Updates 13
Report Launch with Browser 13
Common Issues for SAN and IP 13
Miscellaneous Important Notes that Apply to both SAN and IP Installations 13
Patch Installer troubleshooting 14
SMI Agent 17
Indications delivery depends on SAN Size and SNMP registration 17
Logging for CIMOM 17
Service Location Protocol (SLP) support 17
SLP on UNIX systems 18
SLP on Windows systems 19
Enumeration issue with Brocade 8000 running on Fabric OS 6.3.x or lower 20
Instance class key property with special character 20
Getinstance operation on Brocade_Ethernetport for Fabric OS 6.1.2_CEE 20
FC port type value for imported HBA's 20
Migration Issue 20

Documentation Updates 20
Defects 21
Closed with Code Change in Brocade Network Advisor 11.1.2 21
Closed with Code Change in Brocade Network Advisor 11.1.1 22

Overview

Brocade Network Advisor 11.1 is a software management platform that unifies network management for SAN, IP and converged networks. Network Advisor combines the best of SAN Management from DCFM and the best of IP Management from INM to provide users with an end-to-end view of their entire networking infrastructure. It provides users with a consistent user interface across FC, IP, FCoE / DCB as well as MPLS networks along with custom views and controls based on the users' areas of specialization. Network Advisor provides users with the utmost flexibility in deployment and operational models, including traditional SAN deployments (FC), traditional Ethernet deployments (Access/Aggregation/Core) and end-to-end convergence (FCoE, iSCSI and NAS over DCB). Brocade Network Advisor can be licensed and deployed to manage SAN only, IP only and SAN+IP networks.

Software Feature Overview

SAN and IP Management Feature Enhancements

- DCB Switches Support: Network Advisor allows users to discover and manage DCB Switches both from SAN and IP Tabs.
- Host Views: Host views are supported on both SAN and IP Tabs. Allows users to discover host either using HCM agent or a Virtual Machine Manager (VMM) like vCenter Server.
- Virtualization: Network Advisor now allows users to discover VMs directly from the vCenter.
- Unified VLAN Management: Allows users to configure VLANs across all of the devices managed by Brocade through a single unified VLAN wizard.
- Unified ACL Management: Allows users to consistently define and deploy ACLs across different types of devices.

IP Management Feature Enhancements

Brocade Network Advisor brings forward many capabilities from IronView Network Manager (INM) for IP network management. Network Advisor for IP network management includes a new user interface and a new scalable architecture, along with the following new capabilities:

- Power Center: Allows users to monitor Power Allocation, Power Consumption and various other PoE related parameters. Network Advisor allows users to manage Power Allocation like turning power ON/OFF either manually or on a scheduled basis. Also, allows users to set thresholds and get notified when power related thresholds are exceeded.
- Dynamic Device Grouping: Allows users to create customized device groups that dynamically update so that the users always have the most recent group of all devices that meet the criteria defined for the group.
- 802.1ag Support: Allows users to enable OAM capabilities across various services running on the Service Provider Networks.

SAN Management Feature Enhancements

Brocade Network Advisor brings forward the capabilities found in Brocade Data Center Fabric Manager (DCFM) for SAN management with additional features and enhancements:

- Policy Monitor: Policy Monitor allows users to setup best practices for their network and run a test manually or on a scheduled basis to make sure the network is conforming to the best practices.
- Frame Monitor: Frame monitor provides a monitoring mechanism that allows configuring different thresholds for different type of frames and report events whenever a count for particular frame type crosses its respective threshold.
- D-port: Brocade Network Advisor allows users to run optical and electrical loopback and link traffic tests. Network Advisor also provides digital diagnostics information on 16 G port optics like Temperature, Rx/Tx Power, Bias Current and Supply Voltage.

- **Bottleneck Detection**: Bottleneck Detection allows users to configure the parameters and view the statistics. In addition, when a bottleneck is detected, Network Advisor allows users to view on topology as well as get informed on the affected hosts.
- **Microsoft System Center Operations Manager (SCOM) Management Pack**: Populates Microsoft SCOM with fabric details, switch details, statistics and call home events. This enhancement was introduced on Network Advisor 11.0.0.
- **Selective Server Support Save**: Ability to include / exclude performance and historical events from db while capturing server support save from SMC. This enhancement was introduced on Network Advisor 11.0.0.
- **SAN Size Check**: A popup message is displayed when the discovered port/switch/AG count exceeds the SAN size selected (small/medium/large).
- **MD5 Checksum Validation**: MD5 Checksum validation is done before importing Firmware files into Repository.

Migrations & Upgrades

- ***Network Advisor Upgrades:*** Network Advisor 11.0.x running on the Linux and Windows operating systems can be upgraded to Network Advisor 11.1.x. SAN users may add IP management to Network Advisor 11.1.x for SAN+IP network management with the procurement of the IP functionality. Also, IP users may add SAN management to Network Advisor 11.1.x for SAN+IP network management with the procurement of the SAN functionality.
- ***DCFM Migration:*** DCFM 10.4.x running on the Linux and Windows operating systems can be upgraded to Network Advisor 11.1.x for SAN. DCFM 10.4.x running on the Solaris platform must first migrate to a supported operating system, and then perform the upgrade to Network Advisor 11.1.x for SAN. Prior versions of DCFM would need to be first upgraded to DCFM 10.4.x and then perform the upgrade to Network Advisor 11.1.x. Upgrades from DCFM to Network Advisor 11.1.x for SAN do not require a new software license key. SAN users may add IP management to Network Advisor 11.1.x for SAN+IP network management with the procurement of the IP functionality.
- ***INM Migration:*** IronView Network Manager (INM) needs to be upgraded to Network Advisor 11.0.x and then to Network Advisor 11.1.x. INM 3.3.0x running on the Linux and Windows operating systems would need to upgrade to Network Advisor 11.0.x for IP. INM 3.3.0x running on the Solaris platform must first migrate to a supported operating system, and then perform the upgrade to Network Advisor 11.0.x for IP. Upgrades from INM to Network Advisor 11.0.x for IP do require a new software license key. Users should refer to the INM Migration Guide for a complete list of supported and unsupported data migrations and features. IP users may add SAN management to Network Advisor 11.1.x for SAN+IP network management with the procurement additional features. Note: ACLs and MAC Filters in INM will not be migrated to 11.0.x.

Operating Systems Supported

Operating System (architecture) / Installer	Supported Package
Windows Server 2003 Std SP2 (x86 32-bit) Windows Server 2008 Std (x86 32-bit) Windows XP Pro SP3 (x86 32-bit) Windows 7 Professional (x86 32-bit)	SAN Only, IP Only, SMIA Only, SAN + IP (Professional), SAN + IP (Enterprise medium)
Windows Server 2008 R2 (x86 64-bit) Data Center, Standard and Enterprise Edition	SAN+IP , SAN Only, IP Only , SMIA Only,
RedHat AS 4.8 (x86 32-bit) RedHat Enterprise Linux 5.5 Adv (x86 32-bit) SUSE Linux Enterprise Server 10 SP1, 11 (x86 32-bit) Oracle Enterprise Linux 5.5 (x86 32-bit)	SAN Only, IP Only, SMIA Only and SAN+IP

Operating System (architecture) / Installer	Supported Package
VMWare ESX 4.0, ESX 4.1 and VCenter 4.1 with Guest VMs of: 1. Windows Server 2003 Std SP2 (x86 32-bit) 2. Windows Server 2008 Std (x86 32-bit)	SAN Only, IP Only, SMIA Only, SAN + IP (Professional), SAN + IP (Enterprise medium)
VMWare ESX 4.0, ESX 4.1 and VCenter 4.1 with Guest VMs of: 1. Windows Server 2008 R2 (x86 64-bit) Data Center, Standard and Enterprise Edition 2. RedHat Enterprise Linux 5.5 Adv (x86 32-bit) 3. SUSE Linux Enterprise Server 10 SP1, 11 (x86 32-bit) 4. Oracle Enterprise Linux 5.5 (x86 32-bit)	SAN Only, IP Only, SMIA Only and SAN+IP

Device Platform & Hardware Support Requirements

The following table lists the versions of Brocade firmware supported in this release. Brocade recommends using the *latest* firmware versions in order to get the greatest benefit from the network and network management.

Operating System	Device Type
2.7.01x, 2.7.02x or 2.7.03	BigIron RX
7.1.x and 7.2.x	FastIron CX, FCX-STK, FGS, FGS-STK, FLS, FLS-STK, FESX, FWS
7.1.x and 7.2.x	FastIron SX/SuperX
5.0.x , 5.1.x and 5.2	NetIron CES, CER, MLX, XMR, MLXe
12.1.x[1], 12.2. x[1], and 12.3	ServerIron ADX
10.2.01x and 11.0.x	ServerIron
4.1.x and 4.2.x	TurboIron 24X
4.3.0.0	Wireless Controllers - RFS 4000, RFS 6000, RFS 7000
4.1.0.0	Wireless APs – AP 7131, AP 7131N
2.5.0.0	Wireless APs – AP 5181
4.1.x and 4.1.01x	FastIron FES

Notes: [1] 12.1.0f and 12.2.1 are not supported.

Switch Type SAN Devices – B-Series	
FOS v5.0.x, v5.1.x, v5.2.x, v5.3.x, v6.0.x. v6.1.x, v6.2.x, v6.3.x, v6.4.x and v7.0.0	Brocade 3900 Brocade 3250 Brocade 3850 Brocade 4100 Brocade 7500[1] Brocade 200E Brocade 4900[2] Brocade 5000[3] Brocade AP7600[4] Brocade 300[5] Brocade 5100[5] Brocade 5300[5] Brocade 6510[12] Brocade 8000[9] Brocade 12000 Brocade 24000 Brocade 7800[10] Brocade VA40-FC Brocade Encryption Switch[7] Brocade 48000 with FC4-16, FC4-32 and FC4-482 blades Brocade 48000 with FR4-18i[1] Brocade 48000 with FC4-16IP[2] Brocade 48000 with FC10-6[4] Brocade 48000 with FA4-18 Brocade DCX[6] with FC8-16, FC8-32,FA4-18, and FC8-48 blades Brocade DCX[6] with FR4-18i blades Brocade DCX with FC10-6 blades Brocade DCX[7] with FS8-18 blades Brocade DCX[10] with FCoE10-24 blades Brocade DCX[10] with FX8-24 blades Brocade DCX-4S[8] with FC8-16, FC8-32,FA4-18, FC8-48 and FC8-64 blades Brocade DCX[11] with FC8-64 blades Brocade DCX-4S[8] with FR4-18i blades Brocade DCX-4S[8] with FC10-6 blades Brocade DCX-4S[8] with FS8-18 blades Brocade DCX-4S with FA4-18 Brocade DCX-4S[10] with FCoE10-24 blades Brocade DCX-4S[10] with FX8-24 blades Brocade DCX-4S[11] with FC8-64 blades Brocade DCX 8510-4[12] and DCX 8510-8[12]

Blade Type SAN Devices – B-Series	
FOS v5.2.x, v5.3.x, v6.0.x, v6.1.x, v6.2.x v6.3.x, v6.4.0 and v7.0.0	Brocade 3014 Brocade 3016 Brocade 4020 Brocade 4016 Brocade 4024[1] Brocade 4018 Brocade 4012 Brocade 4424 Brocade 5410[2] Brocade 5450[2] Brocade 5460[2] Brocade 5424[2] Brocade 5470[2] Brocade 5480[2]
Switch Type SAN Devices – M-Series	
M-EOSc 9.6.x, 9.7.x, 9.8.x and 9.9.x	Brocade M6064 and M6140 Brocade M4500 and M4700 Sphereon 3016, 3032, 3216, 3232, 4300, and 4400
M-EOSn 9.6.x, 9.7.x, 9.8.x and 9.9.x	Brocade Mi10K

Notes:

[1] Requires FOS v5.1.0 or higher
[2] Requires FOS v5.2.0 or higher
[3] Requires FOS v5.2.1 or higher
[4] Requires FOS v5.3.0 or higher
[5] Requires FOS v6.1.0 or higher
[6] Requires FOS v6.0.0 or higher
[7] Requires FOS v6.1.1_enc or higher
[8] Requires FOS v6.2.0 or higher
[9] Requires FOS v6.1.2_CEE or higher
[10] Requires FOS v6.3.x or higher
[11] Requires FOS v6.4.0 or higher
[12] Requires FOS v7.0.0

Installing Network Advisor

Installation instructions are provided for the following operating systems:

- Microsoft Windows
- Linux

The Network Advisor Server runs as multiple services on Windows and multiple processes on Linux; and they start automatically after installation.

To install Network Advisor on Windows (Server)

1. Download and extract the zip archive
2. Navigate to the **Windows** folder
3. Execute *install.exe*
4. Follow the instructions to complete the installation.

To install Network Advisor on Linux (Server)

1. Download and extract the tar.gz archive
2. Navigate to the **Linux** folder.
3. Execute *Install.bin* from the File Manager window.
4. Follow the instructions to complete the installation.

To launch the Network Advisor Client

- To launch the Network Advisor Client on the same local machine as the Network Advisor Server, launch the client as follows:

  Windows: Select Start > Programs > Network Advisor 11.1.x > Network Advisor 11.1.x

  Windows:

  - Client can be launched via Desktop icon.
  - Launch command prompt and go to the location "<Install location>/bin" and type "dcmclient"

  Linux:

  - Client can be launched via Desktop icon.
  - Launch terminal and go to the location "<Install location>/bin" and type "sh dcmclient"

  Windows and Linux: Follow the below steps on launching the client from a web browser.

- To launch the Network Advisor Client from a remote host, launch the client as follows:
  Open a browser window and type the Network Advisor server hostname or IP address in the Address field; for example:

  http://NetworkAdvisorServerhost1.companyname.com/

  http://192.x.y.z/

- If when the Network Advisor server was installed, a Network Advisor web server port number was specified (instead of the default 80); you must specify the port number after the hostname or IP address. In the following examples, 8080 is the web server port number:
  http:// NetworkAdvisorServerhost1.companyname.com:8080/

  http://192.x.y.z:8080/

Please note that the required Client Oracle JRE version has now changed to 1.6.0_24. For remote clients, this JRE needs to be installed prior to establishing a server connection.

Installation Notes

1. On Linux, the Brocade Network Advisor installer becomes unresponsive at the 'Initialize Database' step of the Configuration Wizard, if a value lesser than 1024 is provided for the database port.

Important SAN Notes

This section lists information that you should consider before you use Network Advisor 11.1.x.

Miscellaneous Important Notes that Apply to SAN Installations

1. TSB 2011-106-A has been corrected (Manageability servers running DCFM 10.4.0, 10.4.1, 10.4.2, 10.4.3, 10.4.4 or Brocade Network Advisor 11.0.0 run out of application memory if they are managing Brocade 24000 or 48000 directors for several weeks. The result is recurring server restarts)
2. DCFM 10.4.x and Brocade Network Advisor 11.0.x will not be able to manage products running Fabric OS v7.0 and beyond. To mange those products, customers should upgrade the management application first to Brocade Network Advisor 11.1.x before upgrading the products to Fabric OS v7.0.
3. Host based stand-alone SMI agents cannot manage products with Fabric OS v7.0. It requires use of the integrated SMI Agent with Brocade Network Advisor 11.1.x.
4. While running diagnostic port test, it is important to note that selecting more than one port from same switch/blade and running diagnosis on them simultaneously might result in failure. It is recommended to choose only one port at a time from any given switch/blade for running the diagnostic port test.
5. If a fabric has a large zone database or effective zone configuration (~1MB), zoning report generation may fail.
6. If IPv6 is enabled on the Fabric OS switch, as well as the Brocade Network Advisor server host, then IPv6 will be chosen mode of communication between server and switch.
7. When user migrates from the DCFM 10.4.x to Brocade Network Advisor 11.1.x, it is expected the corresponding DCFM application service to be up and running. The GUI message shown when the DCFM server is not running prompts the user to start the Network Advisor service rather than the DCFM application service.
8. When any FOS switch is upgraded from 6.4.x to 7.x.x firmware and downgraded again to 6.4.x, DCFM 10.4.x servers will show caution badge on switches and Discovery status will not reflect the reason for status
9. Firmware upgrade to Brocade 8000 platform using Brocade Network Advisor will be disruptive to I/O on the Brocade 8000 platform.

Removing Switches

If you plan to segment and remove more than two switches from a fabric and you have Historical performance collection enabled then it is recommended that you accept changes after each Switch segmentation from the client rather than doing it together or switch off track fabric changes.

Secure Fabric OS fabrics cannot be discovered from Network Advisor

Network Advisor does not support Secure FOS (SFOS). If you try to discover the fabric, Network Advisor displays an error message that "Discovery Failed". You will have to remove the secure FOS settings and change it back to a normal fabric before discovering it from Network Advisor.

Display of Logical Switches

If you create Logical switches through the Logical Switch dialog box, the Logical switch displays under undiscovered Logical Switch in the existing Logical Switches Panel. You have to rediscover the newly created logical switch fabric.

Destination columns are blank for Brocade Encryption Switch in top talkers dialog

When the Top Talkers dialog box is launched for the Brocade Encryption Switch, the columns 'Destination, Destination port and Destination switch port are sometimes empty..

Firmware Download through SCP Server

If you use the Windows-based SCP Server, firmware download will fail for the switches. It is recommended you use the Linux-based SCP Server.

DCFM to Network Advisor remote migration is not supported

Remote migration is not supported to Network Advisor. It is recommended that you first migrate from DCFM 10.3.x / 10.4.x to another DCFM 10.3.x / 10.4.x server, and then migrate to Network Advisor.

Important IP Notes

Miscellaneous Important Notes that Apply to IP Installations

1. If DCB switches were discovered as a third party device from IP tab in 11.0.x, and if user migrates to 11.1.x, those third party DCB products will be dropped after migration. User can rediscover them from SAN or IP tab as needed.
2. Non-PoE ports such as management ports and stackable ports are displayed incorrectly as PoE capable ports in the Power Center dialog.
3. Each IP product has a System max value that can be configured for various parameters, such as "ip-filter-sys" for ACLs. Network Advisor deployments do not check whether the payload being sent to the device has a number greater than the system-max value. In such deployment scenarios, the deployment may report success even though the number was limited to the system-max value. To ensure successful deployments, make sure the payload being sent is no greater than System max value.
4. On Fast Iron devices, running firmware at 7.0 and earlier, Brocade Network Advisor may not display previously configured MAC filters in the MAC filter configuration dialog. The same issue may be seen with Turbo Iron devices up to firmware to 4.1.x.
5. It is advised not to deploy configurations on control VLANs (e.g. VLAN ID 4091). The device may become unreachable if control VLANs are deleted.
6. When discovering large MPLS networks with more than 2500 (MPLS services, VLL+VPLS) and 5000 LSPs, the Network Advisor server requires a Windows 64-bit server with 6GB memory.

IP Address and Detailed Reports

IP Management Ports will not be consistent with the CLI port naming conventions. These are caused by SNMP index and port name inconsistencies. In some cases, Management ports will not be displayed in the reports.

Properties Dialog Sorting and Selection can map to incorrect port / product

When a user selects the Properties > Ports tab and sorts by any row and selects a port / product column to launch the performance graph or port action, an incorrect port / product may be selected. Workaround is to disable sorting and reselect the column.

Image Backup with SCP

Image backup is not supported using SCP

Linux and Windows OS: INM to INM Server Cloning for Network Advisor Migration

Please refer to INM 3.3.01a release notes on my.brocade.com doc updates.

Boot, Monitor, Firmware Image Updates

Network Advisor does not support boot and firmware upgrade and downgrade for ADX devices running 12.1 or 12.2 *

Configuration Wizard reports an unsuccessful Unified Image deployment when upgrading from 5.0.00b to 5.0.00d on MLX Devices and 05.0.00d to 05.1.00 *

Report Launch with Browser

Launching a report may show an "Expired Session" message. This only happens when the Firefox browser setting is "Show my windows and tabs from last time".

Common Issues for SAN and IP

Miscellaneous Important Notes that Apply to both SAN and IP Installations

1. Privileges related to SAN and IP features are prefixed with 'SAN –'and 'IP –'strings. After migration from an older version, new privilege names will be displayed in the Role Management dialog with these prefixes.
2. The rollover of wrapper log files may cause the server running on Linux to crash. If this issue is encountered, user is required to terminate the dcmsvc process from task manager and restart the server from Server Console.
3. Pre-canned sflow custom reports and CLI configuration templates are lost while migrating from DCFM to Network Advisor 11.0.x (SAN+IP version).
4. If a custom AOR without any host included manually is assigned to a defined user, all hosts are displayed in topology to that user. But deleting/updating hosts will not be reflected in topology for that user till the Client is restarted.
5. If DCB products move from one fabric managed in Brocade Network Advisor to another managed fabric, VLAN Management dialog will not be populated with the configuration for such products.
6. Network Advisor server startup and restart can take up to 10+ minutes to complete.
7. Authentication: Fall back authentication may not work when LDAP server running on Windows 2008 R2 is used as the primary authentication and local database is the secondary authentication. This is because the error code returned is the same for both invalid credential and user not found.
8. When configuring Brocade Network Advisor in SSL enable mode in application configuration wizard, please ensure that both HTTP and HTTPS ports are free and available for Network Advisor. Currently the application checks only if the HTTPS configured port is available and not the HTTP port.
9. There is a change in the driver version 3.0 parsing boot images before import. This caused an import failing in Network Advisor 11.1.0 stating "Invalid boot image code file". The issue is fixed in Network Advisor 11.1.1 but user will see the same issue in the migrated server from Network Advisor 11.1.0 to 11.1.1/11.1.2. To workaround this issue, User needs to remove the boot image files having version number greater than or equal to 3.0 from repository and import again.
10. Port disable/enable operation on physical TE-Ports might fail in below scenarios:
    a. Disabling the virtual FCoE ports of DCB switches of the corresponding physical TE-Ports through CLI/Web Tools.
    b. Removing the FCoE device connected to the ports.

    DCB asset collection will fail if the trunks are configured for the TE-ports. User will not get updates such as port status, lag and trunk information for the DCB switch. User will need to delete the fabric and rediscover it from the discovery dialog to overcome this issue.

11. An FTP transfer from a Brocade Network Advisor Technical Support Repository dialog to a Cerberus FTP Server and an AIX built-in FTP server, does not work.

Patch Installer troubleshooting

Patch installer may not launch if UAC is enabled on a Windows 7/2008/2008R2 Editions. User has to first disable the UAC using the procedure provided in the troubleshooting section of the User Manual and then launch the patch installer.

Windows OS: Brocade Domestic Call home center

To support Brocade Domestic dial-up Call home center with Windows users, add the below entry in the **hosts** file present in \Windows\System32\drivers\etc folder:

"192.168.0.1 Notify1"

Linux OS: SMC - Restarting services after enabling SSL from Options Dialog in RedHat Linux 5

When the setting of SSL fails from the Options dialog box, complete the following steps to enable SSL:

1. Close the client.
2. Stop the services from SMC.
3. Launch the Configuration wizard again and enable SSL from the wizard.
4. Close and launch SMC again.
5. Start services from SMC.
6. Launch the client.

Support Saves may take a long time with large databases

As databases grow larger from Event, sFlow, and Performance Collector data, the support save operation may take a long time to run. Larger databases will promote longer support save operations. Make sure you have a minimum of 20GB disk space for support save and backup operations.

Performance Counter calculation formulas

Counter Name	Type	Protocol used	Source value	Formula
TX	FC	SNMP	.1.3.6.1.3.94.4.5.1.6	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
RX	FC	SNMP	.1.3.6.1.3.94.4.5.1.7	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
TX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
RX	GE	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
TX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.10	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
RX	FCIP	SNMP	.1.3.6.1.2.1.31.1.1.1.6	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
TX	EE Monitors	HTTP	PortRX (variable from the return html file)	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
RX	EE Monitors	HTTP	PortTX (variable from the return html file)	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
TX	HBA, CNA	HCM API	NA	TX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
RX	HBA, CNA	HCM API	NA	RX = (Delta value[1] / (1000 * 1000)) / (Polling interval[2]/1000)
TX	TE	SNMP	. 1.3.6.1.2.1.2.2.1.11 + .1.3.6.1.2.1.31.1.1.1.2 + .1.3.6.1.2.1.31.1.1.1.3	TX = (Delta value[1] / 1000) / (1000 * 1000)
RX	TE	SNMP	. 1.3.6.1.2.1.2.2.1.17 + .1.3.6.1.2.1.31.1.1.1.4 + .1.3.6.1.2.1.31.1.1.1.5	RX = (Delta value[1] / 1000) / (1000 * 1000)
TX% / RX%	FC, GE, FCIP, HBA, CNA	NA	NA	TX% or RX% = ((TX or RX) / ((105000000 * port speed)*(Polling interval[2]/ 1000.00))) * 100 If Utilization is less than 1 then the value is it to 0.0
TX% / RX%	TE	NA	NA	value = (TX or RX) / 10; TX% or RX% = ((value) / ((105000000 * port speed)*(1000/ 1000.00))) * 100 if Utilization is less than 1 then the value is it to 0.0

Counter Name	Type	Protocol used	Source value	Formula
Compression Ratio	FCIP		.1.3.6.1.4.1.1588.4.1.1.4	Compression Ratio = current value/ 1000 Since for compression ratio we will take the current compression ratio value
Receive EOF	TE		.1.3.6.1.2.1.16.1.1.1.5	Receive EOF = Delta value[1] / (1000 * 1000)
Other Counters				Other counters = Delta value[1]

1) Delta value[1]: is the difference of value retrieved between the two consecutive poling cycles.
2) Polling interval[2] : duration between the two polling cycle

Other performance counters

The other counters are listed in the table below:

Counter Name	Type	Protocol used	Source value
CRC Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.40
Signal Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.43
Sync Losses	FC	SNMP	.1.3.6.1.3.94.4.5.1.44
Link Failures	FC	SNMP	.1.3.6.1.3.94.4.5.1.39
Sequence Errors	FC	SNMP	.1.3.6.1.3.94.4.5.1.42
Invalid Transmissions	FC	SNMP	.1.3.6.1.3.94.4.5.1.41
Rx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.33
Tx Link Resets	FC	SNMP	.1.3.6.1.3.94.4.5.1.34
C3 Discard	FC	SNMP	.1.3.6.1.3.94.4.5.1.28
Latency	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.5
Dropped Packets	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.3
Link Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.2
Timeout Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.9
Fast Retransmits	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.10
Duplicate Ack Received	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.11
Window Size RTT	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.12
TCP Out of Order Segments	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.13
SlowStart Status	FCIP	SNMP	.1.3.6.1.4.1.1588.4.1.1.14
CRC Errors	EE Monitors	HTTP	PortCRC (variable from the return html file)

Installation on Network Mounted Drives is not supported

Installation onto a windows network mounted drive is not supported but install is allowed and DB fails to start.

Client disconnects

Under heavy server load or degraded network links, there is a potential for Network Advisor client to get disconnected from the server. Work around is to restart the client.

SMI Agent

1. If SMI client queries CIMOM server for more than one fabric, and if each fabric has a large zone database (~1MB), then Enumerate Instances operation on Brocade_ ZonemembershipsettingdataInZone will fail. In this scenario, it is recommended to use the association traversal approach via Brocade_Fabric to retrieve the larger zone databases.
2. SMI alert indication BRCD60 is not sent out to SMI clients if Fabric OS switches are discovered but SNMP trap registration has failed. Ensure that Brocade Network Advisor server is successfully registered for traps on all switches.
3. If DCB switches are running Fabric OS 6.3.x and 6.3.1_cee, VLAN/ACL deployment through SMI-A will fail. It is required to upgrade the DCB Fabric OS to 6.4.x/6.3.1_dcb/7.0.0 for VLAN/ACL deployment support through SMI Agent.

Indications delivery depends on SAN Size and SNMP registration

The time to deliver the indication will vary based on Network Advisor SAN size selected during installation. If large SAN size is selected, indication delivery time will be longer.

Provider classes may take more time to update the fabric changes if the switches managed in Network Advisor are not SNMP registered. As this would cause a delay in indication delivery, all the switches managed in Network Advisor should be SNMP registered

Logging for CIMOM

The default logging level is "INFO" in integrated Agent. To change the logging level to DEBUG, update the "com.brocade" category value in cimom-log4j.xml file present in <Installation Dir>\conf folder.

The log file size and number of log files also can be changed by modifying the file rolling appender parameters in this cimom-log4j.xml file.

Logging Level, File size and Number of Log files can be changed by modifying the following fields:"Log Level", "File Size" and "Number of Files" from Configuration Tool through CIMOM tab.

Service Location Protocol (SLP) support

The Management application SMI Agent uses Service Location Protocol (SLP) to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

You do not need a WBEM client to use SLP discovery to find a WBEM Server; that is, SLP discovery might already know about the location and capabilities of the WBEM Server to which it wants to send its requests. In such environments, you do not need to start the SLP component of the Management application SMI Agent.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, start the SLP component of the Management application SMI Agent to allow advertisement of its existence, location, and capabilities.

SLP installation is optional and you can configure it during Management application configuration. Once installed, SLP starts whenever the Management application SMI Agent starts.

Management SMI Agent SLP application support includes the following components:

- slpd script starts the slpd platform
- slpd program acts as a Service Agent (SA). A different slpd binary executable file exists for UNIX and Windows systems.
- slptool script starts the slptool platform-specific program

- slptool program can be used to verify whether SLP is operating properly or not. A different slptool exists for UNIX and Windows.

By default, the Management application SMI Agent is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show the Management application SMI Agent:

- accepts WBEM requests over HTTP without SSL on TCP port 5988
- accepts WBEM requests over HTTPS using SSL on TCP port 5989

slptool commands

Use the following slptool commands to verify whether the SLP is operating properly.

- slptool findsrvs service:service-agent
  Use this command to verify that the Management application SMI Agent SLP service is properly running as a Service Agent (SA).

  Example output: service:service-agent://127.0.0.1,65535

- slptool findsrvs service:wbem

Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM services.

Example outputs:

service:wbem:https://10.0.1.3:5989,65535

service:wbem:http://10.0.1.3:5988,65535

This output shows the functionalities of Management application SMI Agent:

- accepts WBEM requests over HTTP using SSL on TCP port 5989
- accepts WBEM requests over HTTP without SSL on TCP port 5988
- slptool findattrs service:wbem:http://IP_Address:Port
  - Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol.
  - Example input: slptool findattrs service:wbem:http://10.0.1.2:5988
  - Note: Where IP_Address:Port is the IP address and port number that display when you use the slptool findsrvs service:wbem command.
- slptool findattrs service:wbem:https://IP_Address:Port
  - Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTPS protocol.
  - Example input: slptool findattrs service:wbem:https://10.0.1.2:5989
  - Note: Where IP_Address:Port is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

SLP on UNIX systems

This section describes how to verify the SLP daemon on UNIX systems.

SLP file locations on UNIX systems:

- SLP log—Management_Application/cimom /cfg/slp.log
- SLP daemon—Management_Application/cimom /cfg/slp.conf
- The SLP daemon can be reconfigured by modifying,
  SLP register—Management_Application/cimom /cfg/slp.reg

You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html

Verifying SLP service installation and operation on UNIX systems:

1. Open a command window.
2. Type % su root and press Enter to become the root user.
3. Type # Management_Application/cimom/bin/slptool findsrvs service:service-agent and press Enter to verify the SLP service is running as a Service Agent (SA).
4. Type # < Management_Application >/cimom/bin/slptool findsrvs service:wbem and press Enter to verify the SLP service is advertising its WBEM services.
5. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
    - Type # Management_Application/cimom /bin/slptool findattrs service:wbem:http://IP_Address:Port and press Enter.
    - Type # Management_Application/cimom /bin/slptool findattrs service:wbem:https://IP_Address:Port and press Enter.

Note: Where IP_Address:Port is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

SLP on Windows systems

This section describes how to verify the SLP daemon on Windows systems.

SLP file locations:

- SLP log—Management_Application\cimom \cfg\slp.log
- SLP daemon—Management_Application\cimom\cfg\slp.conf
  The SLP daemon can be reconfigure the by modifying this file.
- SLP register—Management_Application\cimom\cfg\slp.reg
  statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html

Verifying SLP service installation and operation on Windows systems:

1. Launch the Server Management Console from the Start menu.
2. Click Start to start the SLP service.
3. Open a command window.
4. Type cd c:\Management_Application\cimom \bin and press Enter to change to the directory where slpd.bat is located.
5. Type > slptool findsrvs service:service-agent and press Enter to verify the SLP service is running as a Service Agent.
6. Type > slptool findsrvs service:wbem and press Enter to verify the SLP service is advertising its WBEM services.
7. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
    - Type > slptool findattrs service:wbem:http://IP_Address:Port and press Enter.

- Type > slptool findattrs service:wbem:https://IP_Address:Port and press Enter.

  Note: Where IP_Address:Port is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Enumeration issue with Brocade 8000 running on Fabric OS 6.3.x or lower

Enumeration instance fails for the following classes:

Brocade_EthernetPortLANEndPoint, Brocade_EthernetAdminDomainHostedLanEndPoint, Brocade_EndpointOfNetworkPipe, Brocade_EthernetSwitchHostedLANEndPoint, Brocade_InEthernetLogicalNetwork, Brocade_LANEndpoint, Brocade_PlatformHostedLANEndPoint

When Brocade Network Advisor manages a Brocade 8000 running on Fabric OS 6.3.x or lower, connected to FDMI enabled CNA.

Instance class key property with special character

Getinstance operation fails if the key property value contains semicolon or non printable character.

Getinstance operation on Brocade_Ethernetport for Fabric OS 6.1.2_CEE

Brocade_Ethernetport information could not be fetched through Getinstance operation if CEE switch runs on Fabric OS 6.1.2_CEE

FC port type value for imported HBA's

Brocade_topologyview.AntecedentFCPortType property value corresponding to the imported HBA is shown as L- port.

Migration Issue

Properties configured in the SMI Agent Configuration Tool do not migrate from DCFM 10.4.0 (Solaris) to DCFM 10.4.0 (Windows) through the Copy Data and Settings screen when migrating from DCFM 10.4.0 (Solaris) to DCFM 10.4.0 (Windows) to Network Advisor 11.1.0 (Windows).

Documentation Updates

The most recent Network Advisor 11.1.x documentation manuals are available on the MyBrocade website, http://my.brocade.com. Updates to previously released manuals can also be found at this site.

Defects

Closed with Code Change in Brocade Network Advisor 11.1.2

This section lists the defects with Critical and High Technical Severity closed with a code change in Network Advisor as of November 18, 2011

Defect ID: DEFECT000355813	**Technical Severity:** High
Summary: Call Home notifications are not received for DCX switches, for events with the ID MS-1009.	
Symptom: For events with the ID MS-1009, user will not receive Call Home notifications.	
Feature: FAULT MANAGEMENT	**Function:** ENHANCEMENT
Probability: Medium	
Found in Release: DCFM10.4.0	**Service Request ID:** 631907
Where Else Fixed: GA: BNA11.2.0 GA	

Defect ID: DEFECT000364915	**Technical Severity:** Medium
Summary: Brocade_Switchfcportstats.BBCreditZero property value is incorrectly populated for EOS switches	
Symptom: Incorrect property value will be shown in the 3rd party management application.	
Feature: SMI Agent	**Function:** CIMOM
Probability: Low	
Found in Release: DCFM10.4.0	**Service Request ID:** 644543

Closed with Code Change in Brocade Network Advisor 11.1.1

This section lists the defects with Critical and High Technical Severity closed with a code change in Network Advisor as of August 16, 2011

Defect ID: DEFECT000347713	**Technical Severity:** High
Summary: Allow/Prohibit Matrix – ASM is not set when activating the Active Configuration with Active=Save option enabled in the Active Matrix confirmation dialog.	
Symptom: ASM bit is not set when activating the configuration file.	
Workaround: Close the dialog and reopen it to enable the ASM bit.	
Feature: PDCM	**Function:** USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350309	**Technical Severity:** High
Summary: FICON – Configure cascaded FICON operation failed while setting HIF and no reason is displayed for the failure.	
Symptom: Configure cascaded FICON operation fails.	
Feature: FICON	**Function:** Cascaded FICON Configuration
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350497	**Technical Severity:** High
Summary: SMIA - ModifyRole() method for DCB devices fails to modify the complete rule of an ACL policy	
Symptom: Unable to modify the ACTION field "Permit/Deny" through ModifyRole() invoke method.	
Feature: SMI Agent	**Function:** CEE Switch Support SubProfile
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350532	**Technical Severity:** High
Summary: SMIA - CreateACL/DeleteACL/ModifyACL are deployed successfully to VF enabled DCB devices, but agent returns "Not Supported" error code	
Symptom: ACL deployment done through SMI-A throws "Not Supported" for Virtual fabric enabled DCB devices	
Feature: DISCOVERY (IP)	**Function:** IP Discovery Service
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351606	**Technical Severity:** High
Summary: Boot image update failed with error message for windows and VMware ESX host.	
Symptom: User will not be able to update boot image.	
Feature: HBA Management	**Function:** BIOS Mgmt
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351792	**Technical Severity:** High
Summary: Installer - Installation hangs at 'Initialize Database' when non-default database port number is given in Server Configuration page of Configuration Wizard	
Symptom: User will not be able to complete the installation when the non-default port is used for the database.	
Feature: Installers	**Function:** USABILITY
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000352404	**Technical Severity:** High
Summary: Driver Download: Help dialog is not getting launched in driver repository dialog.	
Symptom: User will not be able to launch the Help dialog for the Driver repository.	
Feature: HBA Management	**Function:** Bulk Driver Configuration
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000353970	**Technical Severity:** High
Summary: Encryption: Add new LUN path does not remember previous settings in the LUN selection screen	
Symptom: User is required to re-apply the LUN setting in the ' LUN view' dialog	
Feature: Encryption	**Function:** CONFIGURATION
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000340676	**Technical Severity:** Medium
Summary: VMM: Duplicate ESX host entries are shown in Product Tree for all the discovered vCenters after the fabric connected to the ESX host is unmonitored and monitored	
Symptom: Duplicate Host entries shown in Product tree	
Feature: VM Support	**Function:** Host Product Tree UI
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000342018	**Technical Severity:** Medium
Summary: FICON – Merge Operation failed with the Error "Internal error occurred - Failed to perform the requested cascaded FICON merge configurations."	
Symptom: Merge operation fails without appropriate message.	
Feature: FICON	**Function:** Cascaded FICON Merge
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000344011	**Technical Severity:** Medium
Summary: VMM: Deleting a vCenter fails when the fabric is unmonitored but a host is still being managed by the vCenter	
Symptom: vCenter deletion fails and error message "Error during delete discovery Internal error" is displayed.	
Workaround: Relaunch the dialog and delete the vCenter	
Feature: VM Support	**Function:** VM Discovery Setup
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000348771	**Technical Severity:** Medium
Summary: Changing Top Talkers from Tx to Rx fails with error	
Symptom: Error (buffering failed) is displayed when changing Top Talker Flows from Tx to Rx.	
Feature: Performance Management	**Function:** Top Talkers
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349188	**Technical Severity:** Medium
Summary: Fabric Binding – Setting SCC policy failed with the reason unable to establish connection to the switch.	
Symptom: SCC policy is not configured on the fabric	
Feature: Fabric Binding & HIF	**Function:** USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349291	**Technical Severity:** Medium
Summary: LSAN Zoning: In LSAN zoning dialog, Alias name is not shown in the WWN-fabric assigned potential member panel	
Symptom: User will not be able to see the alias name in the LSAN Zoning dialog for FAPWWN members	
Feature: ZONING	**Function:** LSAN Zoning Dialog
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000349786	**Technical Severity:** Medium
Summary: Ping or traceroute from FCIP Troubleshooting times out	
Symptom: Ping or traceroute fails when IP interfaces and crossport interfaces are defined on XGE ports.	
Feature: FCIP	**Function:** USABILITY
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350053	**Technical Severity:** Medium
Summary: In Configuration Repository, Duplicate entry is displayed for each device after migrating from Network Advisor 11.0 to Network Advisor 11.1	
Symptom: Duplicate configuration entry is displayed for each device in configuration repository.	
Feature: Migration	**Function:** NONE
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000350271	**Technical Severity:** Medium
Summary: Support save collection for HBA/CNA fails when SSL is enabled.	
Symptom: Support save collection fails.	
Workaround: Use without SSL mode or use standalone HCM with SSL mode.	
Feature: HBA Management	**Function:** HCM Integration
Probability: High	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351026	**Technical Severity:** Medium
Summary: Event Actions are getting triggered for both Syslogs as well as SNMP traps.	
Symptom: All raslog based messages will trigger event actions for SNMP Traps and Syslogs.	
Feature: FAULT MANAGEMENT	**Function:** Event Processing
Probability: Low	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351441	**Technical Severity:** Medium
Summary: The product tree in the event actions dialog shows E Trunk Ports even when UseIfIndex option is not selected.	
Symptom: Cannot create event action while selecting a switch with E Port trunks configured on it.	
Workaround: Provide the IP address in the Provide IP address, WWN, source name text box.	
Feature: FAULT MANAGEMENT	**Function:** Event Processing
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351688	**Technical Severity:** Medium
Summary: Master Log – Incorrect Description and details are displayed for the link failure event.	
Symptom: Incorrect details are displayed in the Master Log event description.	
Feature: FAULT MANAGEMENT	**Function:** Master Log
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000351889	**Technical Severity:** Medium
Summary: Logical Switches – Failed to unbind the addresses from the ports when moved between the logical switches.	
Symptom: Unbind port addresses operation is not successful	
Feature: Virtual Fabrics	**Function:** Partitioning Dialog
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000352018	**Technical Severity:** Medium
Summary: If LKM certificate has value other than Decru the BES will not accept the certificate from DCFM	
Symptom: When attempting to link the BES to an LKM key vault, if the SSL certificate of the LKM has a value other than Decru, Inc. for the Organization field, the BES will not accept the certificate from DCFM. The following error is displayed by DCFM when attempting to import the certificate: The primary key vault certificate is not issued by the key vault vendor. Either the key vault type is set incorrectly, or the wrong certificate has been loaded for the primary key vault.	
Workaround: Use CLI rather than DCFM to import and register the LKM certificate if the value has been changed from Decru to something else.	
Feature: Encryption	**Function:** CONFIGURATION
Probability: Low	
Found in Release: DCFM10.4.2	**Service Request ID:** 601119

Defect ID: DEFECT000352407	**Technical Severity:** Medium
Summary: Customer's log is flooded by SNMPUSM message.	
Symptom: Customer observes many SNMPUSM messages in the DCFM log. Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 07:15:11 CET 2011 Thu Feb 03 07:15:12 CET 2011 Thu Feb 03 07:15:11 CET 2011 Thu Feb 03 07:15:11 CET 2011 2 10412 20:00:08:00:88:29:B6:20 Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 06:42:10 CET 2011 Thu Feb 03 06:42:11 CET 2011 Thu Feb 03 06:42:10 CET 2011 Thu Feb 03 06:42:10 CET 2011 2 10412 20:00:08:00:88:29:B6:20 Info sw7B 137.156.140.100 Security Event SNMPUSM stats not in time window on 137.156.140.100 Thu Feb 03 06:09:09 CET 2011 Thu Feb 03 06:09:09 CET 2011 Thu Feb 03 06:09:09 CET 2011 Thu Feb 03 06:09:09 CET 2011 1 10412 20:00:08:00:88:29:B6:20	
Feature: UNDETERMINED	**Function:** UNDER REVIEW
Probability: Low	
Found in Release: DCFM10.4.1	**Service Request ID:** 599107

Defect ID: DEFECT000352989	**Technical Severity:** Medium
Summary: Master Log: Invalid characters (series of numbers like OID) is displayed in the Description of Master Log Event	
Symptom: User will be shown incorrect description in the Master Log.	
Feature: FAULT MANAGEMENT	**Function:** SNMP Registration
Probability: Medium	
Found in Release: Network Advisor11.1.0	

Defect ID: DEFECT000353735	**Technical Severity:** Medium
Summary: BNA is trying to backup EOS fabrics when backup all fabrics is checked.	
Symptom: BNA will attempt to backup EOS fabrics when backup all fabrics is checked.	
Feature: Configuration Management	**Function:** SAN - Scheduled Backup
Probability: Low	
Found in Release: Network Advisor11.0.0	

Defect ID: DEFECT000353797	**Technical Severity:** Medium
Summary: Moving ICL ports to another logical switch reports an "operation not supported" message when unbind option is selected.	
Symptom: An error message “The indicated partition does not support this operation “ will be displayed.	
Feature: Virtual Fabrics	**Function:** USABILITY
Probability: Low	
Found in Release: DCFM10.4.5	

Defect ID: DEFECT000354536	**Technical Severity:** Medium
Summary: Performance Management - Clear Counters Progress bar does not get closed even after the process is completed	
Symptom: User will be shown the progress bar until the client is closed and relaunched.	
Feature: Performance Management	**Function:** PMService
Probability: Low	
Found in Release: DCFM10.4.5	